

## Design and Implementation of Smart-H Pot: A Custom Intrusion Detection System

Dr. G. Vasavi<sup>1</sup>, G. T. S. Satyanarayana<sup>2</sup>, B. Vivek Sai<sup>3</sup>, B. Chaitanya S. S. Phani<sup>4</sup>

<sup>1</sup>Assistant professor, Dept. of Cybersecurity, Malla Reddy University., Hyderabad, Telangana, India.

<sup>2,3,4</sup>UG Scholar, Dept. of Cybersecurity, Malla Reddy University., Hyderabad, Telangana, India.

**Emails:** vasavi.gotte@gmail.com<sup>1</sup>, satya2a5i@gmail.com<sup>2</sup>, viveksai8840@gmail.com<sup>3</sup>, chaitanyachowdary5722@gmail.com<sup>4</sup>

### Abstract

*In the digital world with all new cyber threats evolving constantly, protecting digital world from unauthorized access with new threats is more important than ever. Traditional Intrusion Detection Systems (IDS) often fail in capturing real-world attacker behavior due to this constant evolving. To fill the gap of evolving, we are introducing Smart-HPot a lightweighted, custom-built IDS that basically uses a honeypot approach to detect and monitor malicious activities in real time. The system provides the services such as SSH and HTTP within a controlled virtual environment, tempting attackers to attack the honeypot and logging their actions without compromising actual infrastructure. Developed using Python's built-in modules like socket and logging, Smart-HPot records interaction data and sends it to Admin Website which is a user-friendly web dashboard powered by Flask, enables admin with real-time threat visualization and tracking. Unlike traditional IDS tools, Smart-HPot will be easy to deploy, resource-efficient, and can be adaptable to different network environments. This design used in it makes it suitable for both small scale organizations and academic research cybersecurity operations. By offering a clear view of attacker's behavior and patterns, Smart-HPot stands as a cost-effective and proactive security measure. The project highlights the importance of deception technology and sets the stage for future enhancements.*

**Keywords:** Attacks Alerts System; Attacks Monitoring System; Deception Technology; Honeypot Security; Logging Attacks.

### 1. Introduction

Smart-HPot is utilizing a combined approach of implementing a honeypot and Intrusion Detection System by hosted in a VMware environment and honeypot system come within a deception technology, capitalizing between these two security measures to enhance the threat detection and response capabilities by creating Admin window and following up the alerts. Smart-HPot provides vulnerable SSH and HTTP services which are fake and used only to trap attackers. Once engaged, the system accurately tracks malicious behavior of the intruder/attacker while triggering real-time alerts and details to admin window which is under the control of the Cyber analysis team. This multi-protocol capability transforms the honeypot into an effective sinkhole for cyber threat analysis. The Smart-HPot is considered to be early form the deception technology,

it's a well-structured cybersecurity strategy that functions as a decoy system to trap the attacker/intruder by simulating vulnerable system and faking service. The main motive of this Smart-HPot's system forge or counterfeit attackers by fake services. These traps are designed to misguiding malicious actors, allowing for the logging attacks and analysis of their behaviors without exposing real world organization systems to harm[8]. By presenting it which appears to be a vulnerable environment, generally honeypots appear to be a vulnerable environment and gather authentic threat intelligence and uncover attack vectors that might otherwise go undetected. This deception-based defense method marks a shift from reactive security measures to a more proactive and insightful approach. Traditional Intrusion Detection Systems

mainly rely on heavily known pattern recognitions, often through signature-based detection. As such systems may fall short while facing a zero-day or evolving threats[1][2]. Honeypots, with their ability to record live attacks, offer a powerful supplement by enabling organizations to understand novel intrusion attempts in real time. When integrated, honeypots and IDS form a sophisticated threat-detection ecosystem which not only detects but also learns from each attack, improving overall security posture[3][4]. This is what differentiates Smart-HPot which is its dual-layered architecture, comprising both deception and detection, thus maximizing security intelligence. The project not only facilitates cybersecurity awareness and ethical hacking research but, can also supports proactive defense planning in Organizations.

## 2. Literature Survey

The Honeypots are used Cyber Sector especially in cyber defense and the analysis of cyber attack/intrusions has been extensively explored in academic research. The Kippo Honeypot (2014) showcased its capability to effectively monitor SSH brute-force attacks[9]. while tools such as Cowrie and Dionaea expanded their variety of attack vectors supported[10]. The initial investigations, such as those conducted by Spitzner (2003), are defined honeypots as security traps[8]. Subsequently research concentrated on the improvement of the deception strategies which are considered to be the basis of trap and decoys systems. However, the majority of the current honeypots systems either depend on the cloud infrastructure or engineered to oversee specific services like SSH[14]. Collectively, datasets such as CICIDS 2017[12] and UNSW-NB15[13] have offered significant insights into real-world attacker/intruder behaviors, contributing to the development of machine learning-based security solutions where the model is trained with previous attacks. Unlike traditional systems, Smart-HPot presents actionable intelligence for researchers and cybersecurity professionals functioning within both Indian and international network environments. Smart-HPot enhances this body of knowledge by providing a lightweight program, self-sustaining honeypot that integrates multi-protocol deception and

real-time alerting functionalities[5].

## 3. System Analysis

### 3.1.Existing System

Traditionally, Intrusion Detection System have primarily used either two methods. They are signature-based or anomaly-based detection methods, the signature-based system which directly focusing on known attack patterns and anomaly-based system mainly detecting deviations from normal behavior. Tools such as Snort and Suricata are the specifically designed to identify recognized attack patterns only. however, but this design can't withstand a zero-day vulnerabilities[6]. Although this machine learning-based IDS can enhance detection capabilities, they frequently result in a high rate of false positives as well[7], which necessitates the use of manual monitoring. Honeypots such as Dionaea and Cowrie offer a certain level of intrusion monitoring; however, they possess limited protocol support and are contingent upon specific network configurations. This limitation make them unsuitable for private organizations[11] and government entities, where data privacy and control are of utmost importance. These challenges underscore the necessity for a localized, deception-based sinkhole that can function independently, delivering insights into attacker behavior without depending on external resources.

### 3.2.Proposed System

Smart-HPot is a specifically designed honeypot-based intrusion detection system that offers a lightweight system, real-time threat detection and alerting system, and adaptive security solution for organizations. In contrast to the traditional signature-based intrusion detection systems, which can frequently encounter difficulties in identifying a new and emerging threats, Smart-HPot serves as an interactive lure, tempting attackers into a controlled VMware environment where their actions can be monitored and logged. This system functions within a VMware environment and accommodates a variety of network protocols, such as SSH and HTTP, which are commonly targeted by cybercriminals. It meticulously records every interaction, capturing essential information such as IP addresses, attempted exploits, and commands executed by attackers. The

data collected helping cybersecurity professionals to identify the intruders/hacking patterns and improve their defensive strategies. A notable feature of Smart-HPot is its capacity to mislead attackers with realistic system responses, creating the illusion that they are interacting with a genuine server. Thus, the developed honeypot system can deliver the real-time alerts and logs of the attacker pattern/behavior to Admin window, the administration of organization can only access the Admin window and analyze the behavior of the attacker/intruder via the logs generated, then the analysis is reported to incident response teams. This project is designed particularly advantageous for organizations, and research institutions, as it for the strengthening cybersecurity measures. By implementing Smart-HPot, organizations can proactively protect against intruder threats, reduce potential via breaches, and enhance security awareness among IT teams of organizations.

### 3.3. Advantages

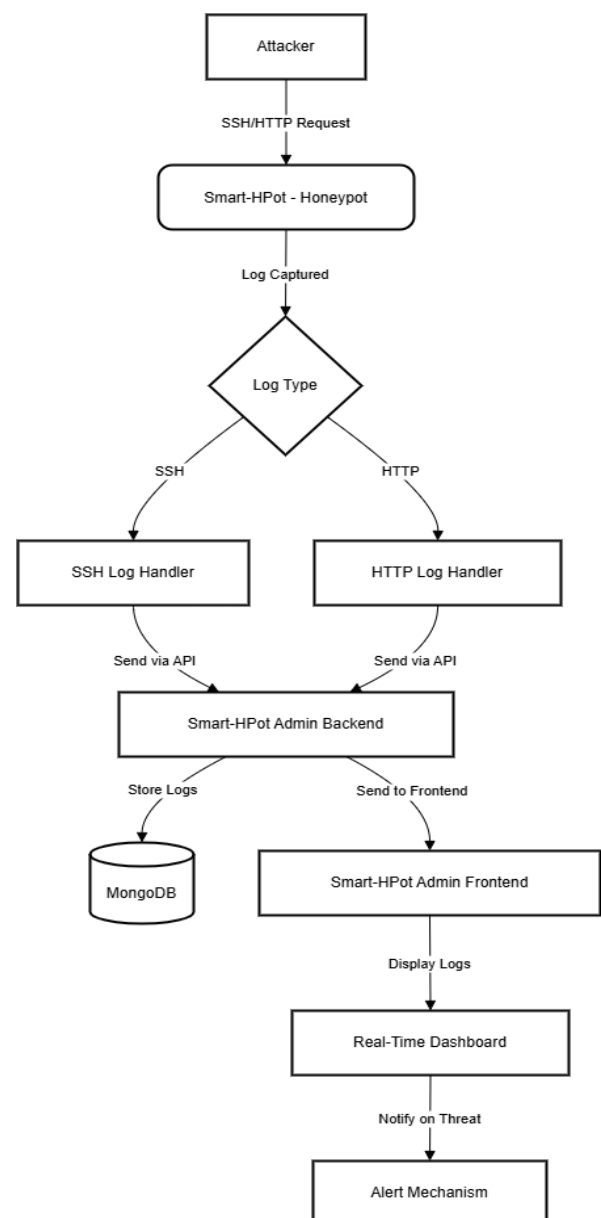
- **Multi-Protocol System:** Generating fake SSH and HTTP services attacks for in-depth examination.
- **Deception Technology:** decoys, traps, make system appear vulnerable and Offer fake services to mislead attackers.
- **Real-Time Alerts System:** Sends immediate alerts and overview of intrusion to Administrator/Incident Response Team via Admin window.
- **Cloud Independence:** Functions in isolated network environments like VMware.
- **Customizability:** Can be customized to meet various security research needs.

### 4. Methodology

The Smart-HPot is an advanced deception-based intrusion detection system specifically designed to capture logs of attacker behavior/ pattern and analyze unauthorized access attempts within a secure virtual environment (VMware). Now the methodology comprises multi-portal, ensuring effective detection, logging, and response to attacks.

- **Attack Initiation** –The process begins when a threat actor intrude(unauthorized) to gain access by sending SSH or HTTP[9] requests to the Smart-HPot.

- **Honeypot Interaction** –The Smart-HPot acts as a decoy, it receives the requests to access and capturing incoming malicious requests and analyzing their features[10].
- **Log Processing & Categorization** –Upon receiving a request, it is categorized into one of two log types:
- SSH Log Tutor processes unauthorized login attempts targeting SSH.
- HTTP Log Tutor documents unauthorized web-based interaction. (Figure 1)



**Figure 1 Methodology**







**Figure 5 Display Analysis**

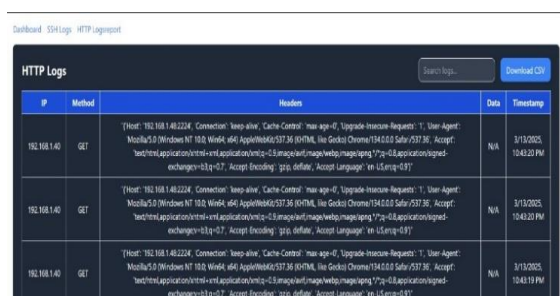
The Admin Window will display all SSH attack logs, which display attacker IP addresses, attempted usernames, passwords, and timestamps. Administrators can review specific logs, can investigate intrusion attempts, and analyze trends as well. Additionally, all logs can be downloaded in CSV/JSON formats for further analysis also. (Figure 6)



IP	Username	Password	Timestamp
127.0.0.1	admin	admin	3/13/2025, 10:23:37 PM
127.0.0.1	admin	admin	3/13/2025, 10:23:37 PM
127.0.0.1	admin	admin	3/13/2025, 10:23:37 PM
127.0.0.1	admin	admin	3/13/2025, 10:23:37 PM
127.0.0.1	admin	admin	3/13/2025, 10:23:37 PM
127.0.0.1	admin	admin	3/13/2025, 10:23:37 PM
127.0.0.1	admin	admin	3/13/2025, 10:23:37 PM
127.0.0.1	admin	admin	3/13/2025, 10:23:37 PM

**Figure 6 Displays all SSH Logs Details**

The Admin Window displays all HTTP attack logs, which displays attacker IP addresses, request headers, dates, and timestamps. Administrators can review specific logs, monitor suspicious activities, and analyze patterns of attackers. It strengthens cybersecurity measures, all logs are available for download in CSV format for further forensic investigation. (Figure 7)

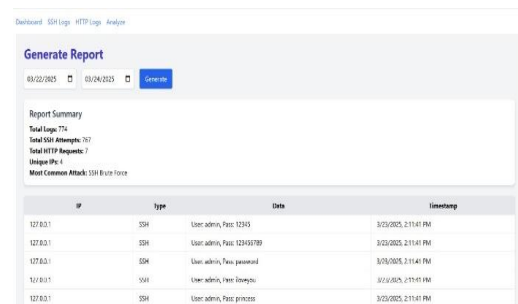


IP	Method	Header	Date	Timestamp
192.168.1.40	GET	"Host: 192.168.1.40; Connection: keep-alive; Cache-Control: max-age=0; Upgrade-Insecure-Requests: 1; User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36;KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36; Accept: */*; text/css,application/javascript,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*; Accept-Language: en-US,en;q=0.7"	N/A	3/13/2025, 10:43:20 PM
192.168.1.40	GET	"Host: 192.168.1.40; Connection: keep-alive; Cache-Control: max-age=0; Upgrade-Insecure-Requests: 1; User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36;KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36; Accept: */*; text/css,application/javascript,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*; Accept-Language: en-US,en;q=0.7"	N/A	3/13/2025, 10:43:20 PM
192.168.1.40	GET	"Host: 192.168.1.40; Connection: keep-alive; Cache-Control: max-age=0; Upgrade-Insecure-Requests: 1; User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36;KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36; Accept: */*; text/css,application/javascript,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml,*/*; Accept-Language: en-US,en;q=0.7"	N/A	3/13/2025, 10:43:20 PM

**Figure 7 Displays All HTTP Logs Details**

Administrators have capability to generate attack report by specifying start and end timestamps in the

Analyze section of the Admin Window. This function allows the extraction of logs for analysis within a designated time period. This provided data consist of attackers IP addresses, Time stamps, Usernames and Passwords/ headers according to report (Figure 8)



IP	Type	Data	Timestamp
127.0.0.1	SSH	User: admin, Pass: 12345	3/13/2025, 2:15:41 PM
127.0.0.1	SSH	User: admin, Pass: 123456789	3/13/2025, 2:15:41 PM
127.0.0.1	SSH	User: admin, Pass: password	3/13/2025, 2:15:41 PM
127.0.0.1	SSH	User: admin, Pass: password	3/13/2025, 2:15:41 PM
127.0.0.1	SSH	User: admin, Pass: password	3/13/2025, 2:15:41 PM

**Figure 8 Analyze and Generate Report**

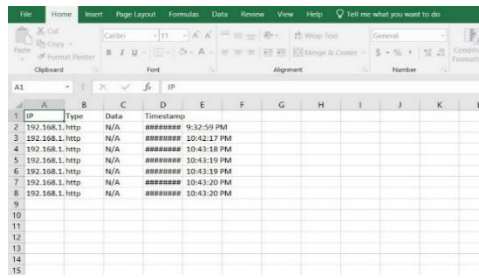
The reports provided in the Analyze section provide a summary of attack logs categorized by specific timestamps. The reports are available in both CSV and JSON formats for further analysis. They have details of SSH and HTTP attempts, unique IP addresses, and prevalent attack types. (Figure 9)



IP	Type	Data	Timestamp
192.168.1.40	http	N/A	3/13/2025, 10:43:19 PM
192.168.1.40	http	N/A	3/13/2025, 10:43:20 PM
192.168.1.40	http	N/A	3/13/2025, 10:43:20 PM

**Figure 9 Download Generated Report in CSV & JSON Files**

The downloaded CSV file contain attackers data, like IP addresses, types of attempts(ssh/http), timestamps, and request details according to attack. This organized format allows administrators to analyze the information with ease, facilitating the of intrusion trends and the enhancement of security measures. (Figure 10) During the process of testing, Smart-HPot proficiently detected and documented SSH brute-force attacks, HTTP directory traversal attempts, and suspicious Telnet activities[11]. The deception-based responses successfully misled the attackers, whilst the real-time alert system offered prompt notifications. The logs generated from the sinkhole disclosed complex patterns of malicious interactions, thereby illustrating its effectiveness as a network defense mechanism[13].



IP	Type	Data	Timestamp
192.168.1.1	http	N/A	10:42:50 PM
192.168.1.1	http	N/A	10:42:17 PM
192.168.1.1	http	N/A	10:43:18 PM
192.168.1.1	http	N/A	10:43:19 PM
192.168.1.1	http	N/A	10:43:19 PM
192.168.1.1	http	N/A	10:43:19 PM
192.168.1.1	http	N/A	10:43:20 PM

**Figure 10 Downloaded Details of Attackers**

## Conclusion

Smart-HPot is an extremely lightweight, deception-based intrusion detection honeypot that effectively monitors cyber threats in real-time. By visualizing vulnerabilities to administrator, it produces detailed attacker logs, to defend organization against the threat actors and also enabling cybersecurity researchers to examine emerging attack patterns as well. Unlike cloud-based honeypots, it ensures data privacy and total control over network security. With its capability to support various protocols, deceptive strategies, and real-time alerts, Smart-HPot acts as a significant asset for ethical hacking research and cybersecurity awareness.

## Future Scope

Smart-HPot can be further enhanced by integrating AI-based detection which can add a weighted advantage to the existing project, and can enables automated troubleshooting as well. Additionally, its functionalities will strengthen ICS/SCADA security system, rendering it significant for the safeguarding of both artificial and critical infrastructure[10]. Therefore, the integration of multiple honeypots can improve collaborative threat intelligence across diverse networks. Predictive analytics driven by machine learning can aid in real-time threat prevention. In India, where awareness of cybersecurity is increasing, Smart HPot can serve as an essential research tool for cybersecurity professionals, ethical hackers, and government entities, facilitating proactive defense against cyber threats[13].

## References

- [1]. Hoque, M. S., Mukit, M. A., & Bikas, M. A. N. (2012). An implementation of intrusion detection system using genetic algorithm. Shahjalal University of Science and Technology, Bangladesh.
- [2]. Kakad, A. R., Kamble, S. G., Bhuvad, S. S., & Malavade, V. N. (2014). Study and Comparison of Virus Detection Techniques. International Journal of Advanced Research in Computer Science and Software Engineering.
- [3]. Khattab, S., Melhem, R., Mossé, D., & Znati, T. (2004). Honeypot back-propagation for mitigating spoofing distributed Denial-of-Service attacks. University of Pittsburgh, USA.
- [4]. Kuwatly, I., Sraj, M., & Al Masri, Z. (2004). A Dynamic Honeypot Design for Intrusion Detection. American University of Beirut.
- [5]. Almotairi, S., Clark, A., Mohay, G., & Zimmermann, J. (2007). A Technique for Detecting New Attacks in Low-Interaction Honeypot Traffic. Queensland University of Technology, Australia.
- [6]. Gupta, B. B., Joshi, R. C., & Misra, M. (2012). Distributed Denial of Service Prevention Techniques. IEEE.
- [7]. Kambow, N., & Passi, L. K. (2014). Honeypots: The Need of Network Security. International Journal of Computer Science and Information Technologies, 5(5), 6098-6101.
- [8]. Spitzner, L. (2003). Honeypots: Tracking Hackers. Addison-Wesley Professional.
- [9]. Kippo Honeypot. (2014). SSH Brute Force Detection and Logging.
- [10]. Cowrie Project. (2009). A Medium-Interaction SSH and Telnet Honeypot.
- [11]. Dionaea Honeypot. (2017). A Low-Interaction Malware Capture Honeypot.
- [12]. CICIDS 2017 Dataset. Canadian Institute for Cybersecurity Intrusion Detection System Dataset. University of New Brunswick.
- [13]. UNSW-NB15 Dataset. A Hybrid Intrusion Detection Dataset for Cybersecurity Research. University of New South Wales.
- [14]. Singh, A., & Sharma, P. Machine Learning for Intrusion Detection Using Honeypots: A Survey. International Journal of Cyber Security.